Specification Information Note

WAP-199_102 WTLS-20010214-a

Version 14-Feb-2001

for

Wireless Application Protocol
WAP-199-WTLS-20000218-a

Wireless Transport Layer Security Specification
Version 18-Feb-2000

This document is considered confidential and may not be disclosed in any manner to any non-member of the WAP Forum™, unless there has been prior explicit Board approval.

This document is a work in process and is not an approved WAP Forum™ specification. This document is subject to revision or removal without notice. No part of this document may be used to claim conformance or interoperability with the WAP Forum specifications.

© 2001, Wireless Application Protocol Forum, Ltd. All Rights Reserved. Terms and conditions of use are available from the WAP Forum™ Web site (http://www.wapforum.org/what/copyright.htm).

© 2001, Wireless Application Protocol Forum, Ltd. All rights reserved.

Terms and conditions of use are available from the WAP Forum™ Web site at http://www.wapforum.org/what/copyright.htm.

You may use this document or any part of the document for internal or educational purposes only, provided you do not modify, edit or take out of context the information in this document in any manner. You may not use this document in any other manner without the prior written permission of the WAP Forum™. The WAP Forum authorises you to copy this document, provided that you retain all copyright and other proprietary notices contained in the original materials on any copies of the materials and that you comply strictly with these terms. This copyright permission does not constitute an endorsement of the products or services offered by you.

The WAP Forum™ assumes no responsibility for errors or omissions in this document. In no event shall the WAP Forum be liable for any special, indirect or consequential damages or any damages whatsoever arising out of or in connection with the use of this information.

WAP Forum™ members have agreed to use reasonable endeavors to disclose in a timely manner to the WAP Forum the existence of all intellectual property rights (IPR's) essential to the present document. The members do not have an obligation to conduct IPR searches. This information is publicly available to members and non-members of the WAP Forum and may be found on the "WAP IPR Declarations" list at http://www.wapforum.org/what/ipr.htm. Essential IPR is available for license on the basis set out in the schedule to the WAP Forum Application Form.

No representations or warranties (whether express or implied) are made by the WAP Forum™ or any WAP Forum member or its affiliates regarding any of the IPR's represented on this list, including but not limited to the accuracy, completeness, validity or relevance of the information or whether or not such rights are essential or non-essential.

This document is available online in PDF format at http://www.wapforum.org/.

Known problems associated with this document are published at http://www.wapforum.org/.

Comments regarding this document can be submitted to the WAP Forum™ in the manner published at http://www.wapforum.org/.

Contents

1. SCOPE **4**

2. NOTATION **4**

3. INTER-SPECIFICATION DEPENDENCIES **5**

3.1 CHANGE CLASSIFICATION 5
3.2 CHANGE SUMMARY 5
3.3 CHANGE DESCRIPTION 5

4. WARNING FOR THE USE OF 40-BIT CIPHERS **6**

4.1 CHANGE CLASSIFICATION 6
4.2 CHANGE SUMMARY 6
4.3 CHANGE DESCRIPTION 6

5. DEFINE OIDS FOR ELLIPTIC CURVES **7**

5.1 CHANGE CLASSIFICATION 7
5.2 CHANGE SUMMARY 7
5.3 CHANGE DESCRIPTION 7

6. ADD REFERENCE DESCRIBING THE SCR SYNTAX **9**

6.1 CHANGE CLASSIFICATION 9
6.2 CHANGE SUMMARY 9
6.3 CHANGE DESCRIPTION 9

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

1. Scope

This document provides changes and corrections to the following document files:

- WAP-199-WTLS-20000218-a

It includes changes from the following change requests:

WTLS-Nokia-Interspec	Inter-specification dependencies
WTLS-VF-Munich-01	Warning for the use of 40-bit ciphers
WTLS-Motorola-Munich-20	Elliptic Curve OIDs

2. Notation

In the subsections describing the changes new text is underlined. Removed text has ~~strikethrough~~ marks. The presented text is copied from the specification. Text that is not presented is not affected at all. The change descriptions may also include editor's notes similar to the one below. The notes are not part of the actual changes and must not be included in the changed text.

Editor's note: Framed notes like these only clarify where and how the changes shall be applied.

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

3. Inter-Specification Dependencies

3.1 Change Classification

Class 3 – Clerical Corrections

3.2 Change Summary

Inter-specification Dependencies

3.3 Change Description

Appendix E:

Add a column 'Requirements' to each of the tables, with no contents.

Add a new item in E.2

Item	Function	Subfunction	Reference	Status	Requirements
WTLS-C220	Use of WIM		[WAP WIM]	O	WTLS-C070, WIM:MCF, WIMME-001

Add a new item in E.2

Item	Function	Subfunction	Reference	Status	Requirements
WTLS-C007		Start negotiation after a cleartext Hello Request	10.5.1.1	O	

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

4. Warning for the use of 40-bit ciphers

4.1 Change Classification

Class 3 – Clerical Corrections

4.2 Change Summary

Warning for the use of 40-bit ciphers

4.3 Change Description

Editor's note: Appendix A, add text above table 1:

Appendix A, add text above table 1:

Warning: 40 bit ciphers are highly susceptible to exhaustive search attacks. It is therefore strongly recommended that they are not used, and ideally, not supported. Servers (but not clients) may need to support 40 bit ciphers for reasons of backward compatibility.

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

5. **Define OIDs for elliptic curves**

5.1 Change Classification

Class 3 – Clerical Corrections

5.2 Change Summary

Define OIDs for elliptic curves

5.3 Change Description

Section 3.1, page 8: add the following reference

[SEC2] "SEC 2: Recommended Elliptic Curve Domain Parameters", Standards for Efficient Cryptography Group, Version 1.0, September 2000. Available from http://www.secg.org/.

Section 3.1, page 8: update the following reference.

[X9.62] "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature

~~**[X9.62] "The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62 Working Draft, September 1998.**~~

Section 3.2, page 8: update the following reference.

[X9.63] "Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", ANSI X9.63-200x Working Draft, October 2000.

~~[X9.63] "Public Key Cryptography for the Financial Services Industry: Key Agreement and Key Transport Using Elliptic Curve Cryptography", ANSI X9.63 Working Draft, October 1998.~~

Appendix A, Table 8, page 84: add the following OIDs before the tables for the predefined curves.

The predefined curves have the following ISO object identifiers corresponding to their assigned numbers:

wap-wsg-idm-ecid OBJECT IDENTIFIER ::= { wap-wsg 4 }

wap-wsg-idm-ecid-wtls1 OBJECT IDENTIFIER ::= { wap-wsg-idm-ecid 1}

wap-wsg-idm-ecid-wtls6 OBJECT IDENTIFIER ::= { wap-wsg-idm-ecid 6}

wap-wsg-idm-ecid-wtls8 OBJECT IDENTIFIER ::= { wap-wsg-idm-ecid 8}

wap-wsg-idm-ecid-wtls9 OBJECT IDENTIFIER ::= { wap-wsg-idm-ecid 9}

Note that the remaining curves have existing ISO object identifiers as follows:

ellipticCurve OBJECT IDENTIFIER ::= { iso(1) identified-organization(3) secg(132) curve (0) }

c-TwoCurve1 OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves (3) charcteristicTwo(0) }

Curve 3 - sect163k1 OBJECT IDENTIFIER ::= { ellipticCurve 1 } in [SEC2]

(also labeled as ansit163k1 in [X9.63])

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

curve 4 - sect113r1 OBJECT IDENTIFIER ::= { ellipticCurve 4 } in [SEC2]

curve 5 - c2pnb163v1 OBJECT IDENTIFIER ::= { c-TwoCurve 1 } in [X9.62]

curve 7 - secp160r1 OBJECT IDENTIFIER ::= { ellipticCurve 8 } in [SEC2]

(also labeled as ansip160r1 in [X9.63])

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved

6 Add reference describing the SCR syntax

6.1 Change Classification

Class 3 – Clerical Corrections

6.2 Change Summary

Add reference describing the SCR syntax

6.3 Change Description

In 3.1, add reference:

[WAPCREQ] "Specification of WAP Conformance Requirements", WAP-221-CREQ, WAP Forum Ltd, URL:http//www.wapforum.org/"

© 2001, Wireless Application Protocol Forum, Ltd.
All rights reserved